Review of Master's Thesis

Student: Pořízek David, Bc.
Title: Transparent Encryption Solution for Endpoint Devices (id 22055)
Reviewer: Ryšavý Ondřej, doc. Ing., Ph.D., UIFS FIT VUT

1. Assignment complexity — **average assignment**

Zadání požadovalo vytvoření konkrétního řešení transparentního šifrování pro platformu MS Windows. Zásadní pro práci bylo porozumění souborového systému a principu použití Minifilter Framework.

2. Completeness of assignment requirements — **assignment fulfilled**

3. Length of technical report — **in usual extent**

4. Presentation level of technical report — **70 p. (C)**

Práce v první části obsahuje úvod do problematiky, analýzu požadavků a uvažovaných použití nástroje. V další části se pak jedná o návrh nástroje a popis jeho implementace, na kterou navazuje kapitola o testování a ověření vlastností. Samotný popis návrhu a implementace nástroje je poněkud strohý a uvádí informace, které se spíše týkají použitých prostředků. Popis v kapitole Encryption Header je matoucí. Zejména informace o tom, že content key se generuje při každém požadavku. Také zde uvedený popis neodpovídá obrázku 6.1. V práci není příliš prostoru věnováno vysvětlení, jak se použijí šifrovací algoritmy, například v jakém režimu byl použit algoritmus AES.
Práce dále obsahuje některé zvlášnosti, které snižují její kvalitu, například, kapitola 2.4 začíná varováním, že může obsahovat nepravdivé informace.

5. Formal aspects of technical report — **85 p. (B)**

Práce je psána anglicky na dobré úrovni. V práci se místy objevují typografické či jazykové nedostatky, například:

- " ...network. [18]"
- "appending" -> "prepending" na str. 36
- "...enough to the time"

6. Literature usage — **80 p. (B)**

V práci byly použity převážně on-line zdroje, což je vzhledem k charakteru řešeného problému pochopitelné. Nicméně není uveden žádný zdroj z oblasti kryptografie, přestože šifrování se objevuje v názvu práce. Převzaté informace jsou v textu dostatečně odlišeny.

7. Implementation results — **75 p. (C)**

Realizační výstup je funkční pro většinu případů. Vytvoření ovladače pro operační systém není triviální úkol a autor jej velmi dobře zvládnul. Implementace byla otestována a její výkon vyhodnocen pomocí ručních a automatických testů. Je otázkou, zda nebylo možné navíc využít některé z existujících testovacích nástrojů, například "Installable File System Filter Test".
Autor zmiňuje chybu při manipulaci s MPEG soubory. Spíše než formát samotný je problém v aplikaci, které k tomuto souboru přistupují. Nalezení a odstranění této chyby je nutné a nemělo by být označeno jenom za nežádoucí "vlastnost".
Pro zabezpečení dat se vytváří nová hlavička, která se vkládá na začátek souboru, což je inspirováno řešením firmy ESET. Otázkou zní zda je toto vhodný přístup. Modifikace velikosti souboru a hlavně posunutí jeho začátku způsobuje množství problémů, které zesložiťují implementaci ovladače. Pro tuto hlavičku by bylo možné použít alternate data stream v případě NTFS, či extra souboru s metadaty pro FAT.

8. Utilizability of results

Výsledek práce má být použit v systému DLP komerčního subjektu. Vzhledem k tomu, že produkt není plně funkční bude potřeba nejprve chybu nalézt a opravit.

9. Questions for defence

- Vysvětlete větu uvedenou v rozšířeném abstraktu co "...systém k souboru přistoupí většinou dříve, než si jej uživatel reálně vyžádá."
- Na straně 13 popisujete případ použití uvažovaného systému. V bodě 7 tvrdíte, že uživatel při kopírování dostane pouze zašifrovaný soubor, zatímco když jej otevře tak uvidí jeho nešifrovaný obsah. Jak je to možné?

- Testoval jste také případy, kdy je použit přístup Memory Mapped Files?
- Jaký význam má encryption header identificator? Je z něj možné zjistit verzi, respektive použitý šifrovací algoritmus?

10. Total assessment

75 p. good (C)

Jedná se o zajímavou práci s praktickým potenciálem. Tvorba ovladače není jednoduchá záležitost, ale byla studentem zvládnuta. Před praktickým použitím bude vhodné ovladač důkladněji otestovat a hlavně najít a opravit uvedenou chybu. Text práce obsahuje podstatné informace. Samotný popis řešení místy nenabízí dostatek informací o způsobu zabezpečení dat či analýzu alternativních přístupů a jejich vyhodnocení. Celkově se nicméně jedná o povedenou práci.

In Brno 4. June 2019

Ryšavý Ondřej, doc. Ing., Ph.D.
reviewer